

Lesson 7. Banking and Credit Card Security

Lesson Purpose

To focus on protecting access to private financial information when banking or using ATMs and credit cards.

Learning Objectives

Participants will be able to:

- Identify common ways that thieves get access to financial information.
- Describe general strategies for preventing thieves from getting personal financial information.
- Identify specific strategies for protecting financial information when using ATMs and credit cards.
- Describe procedures for monitoring your credit record and correcting errors detected.

Materials

Presentation: Banking and Credit Card Security

Handout(s): *"Safe and Secure in an Electronic World"*

Supplement: *"Automated Teller Machine Safety,"* from the National Crime Prevention Council. Download at www.ncpc.org

Display sample bank account and credit card statements that include private financial information.

Related Resources

National Crime Prevention Council, www.ncpc.org

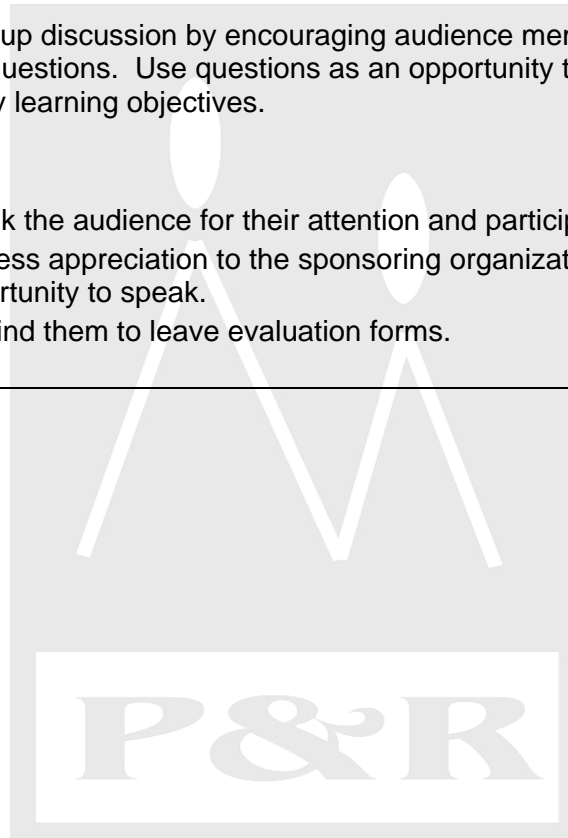
Lesson Plan

Time	Main Points	Slide
	Introduction	
5 min.	Enterprising criminals can gather enough information about you through the debris of everyday electronic transactions to pretend that they are you. Once this happens, they can gain access to all of your financial information. The most common way thieves go about getting this information is by stealing your wallet. However, other ways include looking over your shoulder at ATMs and phone booths to capture your PIN number, stealing mail from your mailbox, digging through your discarded trash and fraudulently ordering a copy of your credit record.	1 - 2
	Briefly describe a local example of banking/credit card fraud.	

Time	Main Points	Slide
	Today, we will look at ways that thieves get access to financial information, review some general and specific strategies for preventing them from getting your information, and explain how you can monitor your financial information and correct errors.	
	Distribute handout: <i>"Safe and Secure in an Electronic World"</i>	
Presentation		
3 min.	How criminals get your private financial information -- Most common - stealing your wallet. Also: <ul style="list-style-type: none"> Looking over your shoulder at ATMs and phone booths to capture your PIN number. Stealing mail from your mailbox. Digging through your discarded trash. Fraudulently ordering a copy of your credit record. 	3
6 min.	To prevent this from happening to you, <ul style="list-style-type: none"> Don't give out your Social Security number. Tear into small pieces all credit card offers, ATM receipts, bank statements, credit card statements and other printed materials that have your account numbers on them. Don't send personal information over the Internet, through e-mail or over cellular phones. Don't use passwords that are obvious. Change your password regularly and memorize it. 	4
3 min.	Pay Particular Attention When Using ATM Cards and Credit Cards Protecting Your Personal Identification Number (PIN) <ul style="list-style-type: none"> A PIN is a confidential code issued to you that lets you have access to your account. Memorize your PIN, and don't give it to anyone, not even family members or bank employees. Never write your PIN on your ATM card or write it on a piece of paper and place it in your wallet. If your wallet or card is ever lost or stolen, someone who finds it will have everything they need to take all the money from your account. 	5
4 min.	Using the ATM Safely An ATM card should be treated like cash. When using the ATM machine, select one that's code-door or double-door secured and visible to street traffic. Use when others are around. Also, <ul style="list-style-type: none"> Be aware of others waiting behind you. Position yourself in front of the keyboard to prevent anyone from seeing you enter your PIN. 	6

Time	Main Points	Slide
	<ul style="list-style-type: none"> ▪ Be courteous while waiting by keeping a polite distance from the person ahead of you. Allow the person to finish his or her business before approaching the machine. ▪ Remove the cash as soon as the machine releases it. Put the money in your pocket and wait until you are in a secure location before counting it. ▪ Never leave the receipt at the site. 	7
4 min.	Protecting Your Credit Cards <ul style="list-style-type: none"> ▪ Give your credit card account number out to make a purchase or reservation only when you have initiated the call. Never give this information over a cellular phone. ▪ Never give your credit card for someone to use on your behalf. ▪ Watch your card when giving it to store clerks to protect against extra imprints being made. 	8
	<ul style="list-style-type: none"> ▪ Destroy any carbon papers from receipts. Tear them up—don't toss them into the trash at the purchase counter. Keep the actual charge slips in a safe place. ▪ Save all receipts and compare them to your monthly statement. Report any differences immediately. ▪ Keep a master list of all your card numbers in a secure place, with all account numbers and phone numbers for reporting stolen or lost cards. ▪ Immediately report lost or stolen cards to the issuing company and to the police. 	9
2 min.	Summarizing <ul style="list-style-type: none"> ▪ Enterprising criminals can gather enough information about you to gain access to all your financial information. ▪ To prevent this from happening to you, protect your private financial information, passwords and PINS. Stay aware whenever using ATMs or credit cards, destroy receipts, scrutinize your credit card and bank statements. 	10
Practice/feedback		
10 min.	<p>Have participants review the list of tips for banking and credit card security in their handout. Ask them to place a checkmark (✓) beside the things they now do and to place an asterisk (*) beside the things that they need to begin to do.</p> <p>Give participants 5 to 7 minutes to complete this review. The instructor should circulate among participants during this time. Conclude the activity by asking 2 or 3 volunteer participants to share what they learned from the review. The instructor should reinforce prevention strategies and key learning points.</p>	11

Evaluation		
10 min.	<p>Set-up</p> <p>We have a few minutes for questions and additional discussion. While we're doing that, we have a brief evaluation form we would like for you to complete and leave with us. Your name is not required, but your feedback is very important. It will help us improve our presentation and program.</p> <p>Distribute evaluation forms and ask for questions or additional comments on what has been presented.</p> <p>Promote group discussion by encouraging audience members to help respond to questions. Use questions as an opportunity to clarify and reinforce key learning objectives.</p> <p>Wrap-up</p> <ul style="list-style-type: none"> ▪ Thank the audience for their attention and participation. ▪ Express appreciation to the sponsoring organization for the opportunity to speak. ▪ Remind them to leave evaluation forms. 	12



7. Banking and Credit Card Security

Please tell us what you think about this lesson by circling the numbers that most closely reflect your opinions.

After this lesson . . .	Strongly Disagree	Disagree	Agree	Strongly Agree
a) I am better able to recognize common ways that thieves get access to financial information.	1	2	3	4
b) I know more strategies to keep thieves from getting personal financial information.	1	2	3	4
c) I know more strategies for protecting financial information when using ATMs and credit cards.	1	2	3	4
d) I am now more likely to monitor my credit report regularly and to report anything suspicious.	1	2	3	4
About this lesson . . .				
e) The information presented was valuable.	1	2	3	4
f) The lesson was presented in a clear and understandable manner.	1	2	3	4
g) Lesson activities and discussion were helpful.	1	2	3	4
h) I would recommend this lesson to others.	1	2	3	4

What was the most valuable thing you learned?

Please give one example of how you plan to use the information presented in this lesson.

How could this lesson be improved?

